

1 CLAIMS

2

3 1. A programmable logic device (PLD) comprising:
4 configurable logic configured by a configuration memory;
5 structure for receiving a bitstream from a source external to the PLD,
6 wherein the bitstream includes unencrypted configuration bits and
7 encrypted configuration bits;
8 a key memory for storing a decryption key;
9 a decryptor having a decryption algorithm for decrypting the encrypted
10 configuration bits in the bitstream using the key, and thereby
11 forming configuration data; and
12 structure for loading the configuration data into the configuration memory.

13

14

15 2. The PLD of Claim 1 wherein the unencrypted configuration bits are control bits
16 and the encrypted configuration bits are configuration data bits.

17

18 3. A programmable logic device (PLD) comprising:
19 configurable logic configured by a configuration memory;
20 structure for receiving a bitstream from a source external to the PLD;
21 a key memory for storing a decryption key;
22 a decryptor having a decryption algorithm for decrypting data in the
23 bitstream using the key;
24 structure for loading the decrypted data into the configuration memory;
25 structure for reading header information from the bitstream indicating
26 whether the bitstream includes encrypted data; and
27 structure for directing the bitstream to the decryptor if the header
28 information indicates the bitstream includes encrypted data and
29 bypassing the decryptor if the header information indicates the
30 bitstream does not include encrypted data.

1

2 4. The PLD of Claim 3 further comprising:

3 structure for reading back configuration from the configuration memory;

4 and

5 structure for disabling the structure for reading back configuration when

6 the header information indicates the bitstream includes encrypted

7 data.

8

9 5. The PLD of Claim 3 further comprising:

10 structure for reconfiguring the PLD after the PLD has been configured; and

11 structure for disabling the structure for reconfiguring the PLD when the

12 header information indicates the bitstream includes encrypted data.

13

14 6. A programmable logic device (PLD) comprising:

15 configurable logic configured by a configuration memory;

16 structure for receiving a bitstream from a source external to the PLD;

17 a key memory for storing a plurality of decryption keys, wherein the key

18 memory includes a plurality of registers for storing the plurality of
19 decryption keys;

20 a decryptor having a decryption algorithm for decrypting data in the

21 bitstream using at least one of the keys; and

22 structure for loading the decrypted data into the configuration memory.

23

24 7. The PLD of Claim 6 wherein the decryptor reads from one of the registers for

25 storing a plurality of decryption keys a value indicating whether another key will

26 also be used for decryption.

27

28 8. The PLD of Claim 6 wherein the decryptor includes a circuit for aborting

29 decryption if an attempt is made to use the keys differently from the way specified

30 by the keys.

1

2 9. The PLD of Claim 6 wherein a key specifies whether it is a first, middle, last, or
3 only key of a key set.

4

5 10. The PLD of Claim 6 wherein a key specifies whether it is a last key or not a last
6 key of a key set.

7

8 11. The PLD of Claim 6 wherein the PLD reads an address of a key from the
9 bitstream.

10

11 12. The PLD of Claim 6 wherein a first group of words in the bitstream is
12 encrypted with a first key known to a first designer and a second group of words
13 in the bitstream is encrypted with a second key known to a second designer.

14

15 13. The PLD of Claim 1 further comprising structure for placing the key memory
16 into a secure mode and a non-secure mode, and wherein keys are loaded while the
17 key memory is in the non-secure mode.

18

19 14. The PLD of Claim 13 wherein the keys can be read while the key memory is in
20 the non-secure mode.

21

22 15. The PLD of Claim 14 wherein moving the key memory from the secure mode
23 to the non-secure mode causes all keys to be erased.

24

25 16. The PLD of Claim 15 wherein moving the key memory from the secure mode
26 to the non-secure mode also causes the configuration data to be erased.

27

28 17. The PLD of Claim 1 wherein the bitstream comprises a plurality of words of
29 data, and the decryption algorithm uses both the key and a previously decrypted

1 word of the configuration data for decrypting a current word of the encrypted
2 configuration bits.

3

4 18. In a PLD having a decryptor for decrypting an encrypted bitstream and a
5 plurality of keys for use by the decryptor, a method of using the plurality of keys
6 comprising:

7 providing a first key to a first designer for encrypting a first part of a
8 design; and

9 providing a second key to a second designer for encrypting a second part of
10 the design.

11

12 19. In a PLD having a decryptor for decrypting an encrypted bitstream and a key
13 for use by the decryptor, a method of using the PLD comprising:

14 placing the PLD into a non-secure mode; and
15 loading the key into the PLD.

16

17 20. The method of using the PLD of Claim 18 further comprising:

18 placing the PLD into a secure mode after the step of loading the key.

19

20 21. In a PLD having a decryptor for decrypting an encrypted bitstream and a key
21 for use by the decryptor, a method of using the PLD comprising:

22 placing the PLD into a non-secure mode;
23 loading the key into the PLD; and
24 operating the PLD in a non-secure mode.

25

26 22. The method of using the PLD of Claim 21 comprising:

27 placing the PLD into a secure mode after the step of operating the PLD in a
28 non-secure mode.

29

30

- 1 23. The method of using the PLD of Claim 21 comprising the further step of:
2 generating a CRC checksum using a bitstream being loaded into the PLD.
3
- 4 24. The method of using the PLD of Claim 21 comprising the further steps of:
5 loading a bitstream including encrypted data into the PLD;
6 decrypting the encrypted data to generate configuration data; and
7 calculating a CRC checksum on the configuration data.
8
- 9 25. The method of using the PLD of Claim 21 comprising the further steps of:
10 loading a bitstream including encrypted data into the PLD;
11 calculating a CRC checksum on the encrypted data; and
12 decrypting the encrypted data to generate configuration data.
13
- 14 26. A programmable logic device (PLD) comprising:
15 configurable logic configured by a configuration memory;
16 structure for receiving a bitstream from a source external to the PLD;
17 a key memory for storing a decryption key;
18 a decryptor having a decryption algorithm for decrypting encrypted
19 configuration bits in the bitstream using the key, and thereby
20 forming configuration data; and
21 structure for loading the configuration data into the configuration memory.
22
- 23 27. The PLD of claim 26 wherein the structure for loading the configuration data
24 into the configuration memory includes a CRC checksum calculation circuit.